NEW UPPER BOUNDS ON THE SPREADS OF THE SPORADIC SIMPLE GROUPS

BEN FAIRBAIRN

ABSTRACT. We give improved upper bounds on the exact spreads of many of the larger sporadic simple groups, in some cases improving on the best known upper bound by several orders of magnitude.

Keywords: exact spread, sporadic simple group
MSC: 20D08, 20C15

1. INTRODUCTION

Recall that a group is said to be 2-generated if it is generated by just two of its elements. Every finite simple group is 2-generated (see [1]) and many authors have considered the question of how easily a pair of elements generating a simple group may be obtained. One quantity measuring this introduced by Brenner and Wiegold in [6] and motivated by earlier work of Binder [2] is the concept of the spread of a group.

Let G be a group. We say that G has *spread* r if for any set of distinct non-trivial elements $X := \{x_1, \ldots, x_r\} \subset G$ there exists an element $y \in G$ with the property that $\langle x_i, y\rangle = G$ for every $1 \leq i \leq r$. We say that this element y is a *mate* of X and that G has *exact spread* *s(G):=r* if G has spread r but not $r + 1$.

The concept of spread is also of interest to computational group theorists since it is useful in the the analysis of the celebrated product replacement algorithm for producing random elements of groups [11]. The concept is also of interest when studying the generating graph of a group [13, Section 4].

The exact spreads of the finite simple groups have been much studied [2, 6, 7, 12]. In particular, bounding the value of the exact spreads of the sporadic simple groups has recently been investigated by several different authors [3, 4, 9, 15] and it is these cases that we focus on here. More specifically we prove the following.

Theorem 1. *The exact spreads of the sporadic simple groups are bounded by the values given in Tables 1 and 2.*

Most of the bounds listed in Tables 1 and 2 are not new. The upper bounds given in Table 1 were obtained by Bradley and Holmes in [3] using coverings of a group by sets of proper subgroups and as such

TABLE 1. Bounds on $s(G)$ for the smaller sporadic simple groups. The upper bounds are proved in [3]. The lower bound for M_{11} is proved in [3, 15]. All other lower bounds are proved in [7]. (Note that aside from M_{11}, M_{12} and J_2 the lower bounds stated in [3, Table 1] are incorrect.)

G	Upper bound Lower bound	G	Upper bound Lower bound
M_{11}	3 3	J_3	597 76
M_{12}	9 3	M_{24}	56 11
J_1	179 76	McL	308 70
M_{22}	26 20	He	1223 198
J_2	24 5	Suz	956 40
M_{23}	8064 8063	Co_3	1839 98
HS	33 18	Fi_{22}	186 13

are unable to handle the sporadic simple groups with very large coverings, which is essentially the larger groups. Our methods are unable to improve upon these bounds.

What is new here are the upper bounds listed in Table 2 for almost all the groups that the methods of [3] could not deal with (our approach does not work for the Baby Monster $\mathbb{B}$, see Section 2.2).

The bounds given in Tables 1 and 2 are, as far as the author is aware, the best known, accepting that Bradley and Holmes claim that for the groups they considered "better results were obtained for some of the groups in trial runs, but our table gives only the results that were given by known seeds" [3, p.138].

In Section 2 we will introduce some preliminary ideas that we will use to prove our bounds in Section 3 in every case aside from the Monster group that we shall deal with separately in Section 4.

2. PRELIMINARIES

In this section we shall describe some concepts that will be useful in proving Theorem 1.

Table 2. The best previous upper bounds for the larger sporadic groups proved in [4]; the new upper bounds proved here and the lower bounds proved in [7]. Note that the seemingly better lower bound given in [9] for HN (10999) is incorrect - see [7, Section 4.7].

G	Old upper bound New upper bound Lower bound	G	Old upper bound New upper bound Lower bound
Ru	12990752 1252799 2880	Th	103613642531 976841774 133997
O'N	5960127 2857238 3072	Fi_{23}	8853365473 31670 911
Co_2	5240865 1024649 270	Co_1	58021747714 46621574 3671
HN	229665984 74064374 8593	J_4	251012689269463297 47766599363 1647124116
Ly	112845651178977 1296826874 35049375	Fi_{24}'	30916396779874577216 7819305288794 269631216855
$\mathbb{B}$	3843675651630431666542962843030 - 174702778623598780219391999999		
$\mathbb{M}$	14587804270839626161268024115186834207944682668030 5791748068511982636944259374 3385007637938037777290624		

2.1. **Support.** Let G be a group and let $x \in G^\#$ where $G^\# := G \setminus \{e\}$. We define the *support* of x to be the set

$$supp(x) := \bigcup_{H<G, x\in H} H^\#.$$

In other words $y \in supp(x)$ means that y is an element of $G^\#$ that lies in a proper subgroup containing x and so y cannot be a mate for the set $\{x\}$. We extend this to subsets $X \subset G^\#$ as follows:

$$supp(X) := \bigcup_{x\in X} supp(x).$$

If $Y \subset supp(X)$ we say that X *supports* Y. In particular, elements of $supp(X)$ cannot be a mate to X.

Table 3. Support classes for the sporadic simple groups.

G	Class	G	Class	G	Class	G	Class
M_{11}	2A	J_3	2A	O'N	2A	Th	2A
M_{12}	2A	M_{24}	2A	Co_3	2A	Fi_{23}	2A
J_1	2A	McL	2A	Co_2	2B	Co_1	2A
M_{22}	2A	He	2A	Fi_{22}	2A	J_4	2B
J_2	2A	Ru	2B	HN	2B	Fi'_{24}	2B
HS	2A	Suz	3A	Ly	2A	$\mathbb{M}$	2B

2.2. **Support classes and characters.** Continuing the earlier nomenclature, we say a conjugacy class $\mathcal{C} \subset G$ is a *support class* if the set $\mathcal{C}$ supports the set $G^{\#}$. For each of the bounds that we improve upon here, our improved bound is obtained by showing that some small conjugacy class of G is a support class.

Note that not every simple group has a support class e.g. the Baby Monster has no support class as the only maximal subgroups with elements of order 47 are copies of the Frobenius group 47:23, but no proper subgroup containing elements of order 23 contains elements of order 31 - see the list of maximal subgroups given in [14] (the list given in [8] is incomplete). This is why we are unable to improve upon the best known bounds in this case.

To obtain a set of elements that has no mate, and thus provide an upper bound on the spread, it is sufficient to take one generating element from each cyclic subgroup generated by an element of a support class. We thus have the following easy lemma.

Lemma 2. *Let $\mathcal{C} \subset G^{\#}$ be a support class, $d := |\langle g \rangle \cap \mathcal{C}|$ for $g \in \mathcal{C}$. Then $s(G) + 1 \leq |\mathcal{C}|/d$.*

Given a conjugacy class $\mathcal{C} \subset G^{\#}$ we define its *support character* $\chi_{\mathcal{C}}$ to be the sum of the primitive permutation characters of G that are nonzero on $\mathcal{C}$. Since the transitive permutation character $1 \uparrow_H^G$ is nonzero at a class $\mathcal{C}$ if and only if $\mathcal{C} \cap H \neq \emptyset$ we have the following lemma.

Lemma 3. *A conjugacy class $\mathcal{C} \subset G^{\#}$ is a support class if and only if $\chi_{\mathcal{C}}(g) > 0$ for every $g \in G$.*

3. Computing the bounds

Our new upper bounds are obtained by finding a small support class using Lemma 3 and then using this to obtain a bound using Lemma 2. This is easily done using the GAP algebra system [10]; first by obtaining the primitive permutation characters using standard GAP functions (primarily the GAP character table library and the tables of marks), then obtaining the support characters (if any) using this data and finally by reading off the support class that gives the best bound from the list just obtained.

The support classes giving the best bound found in this way are given in Table 3. For completeness we give these support classes for each of the sporadic groups that possesses one, that is every sporadic simple group aside from the Mathieu group M_{23} and the Baby Monster $\mathbb{B}$.

For example, in several cases (M_{11}, J_1, M_{22}, M_{23}, J_3, McL, O'N and Ly) there is only one class of involutions and every maximal subgroup has even order (see [8]) so the support character χ_{2A} is the sum of every primitive permutation character and is therefore positive on every class. The class 2A is therefore a support class in these cases by Lemma 3. Note that whilst the Thompson group, Th, also has only one class of involutions it also has a class of maximal subgroups of odd order isomorphic to the Frobenius group 31:15. The elements of this subgroup can easily be seen to also belong to other maximal subgroups with structure $2^5.L_5(2)$ (see [8, p.70]). The support character χ_{2A} is thus equal to the sum of every primitive permutation character, aside from the one defined by the maximal copies of 31:15, and $\chi_{2A}(g) > 0$ for every $g \in \mathrm{Th}$. Thus 2A is a support class by Lemma 3.

4. The Monster

The Monster group $\mathbb{M}$ requires special attention - the methods of previous sections cannot be applied as easily in this case since, at the time of writing, the maximal subgroups of $\mathbb{M}$, and thus the primitive permutation characters of $\mathbb{M}$, have yet to be classified.

All not lost! We can still find a support class in this case using information about its conjugacy classes and the known maximal subgroups.

Lemma 4. *Class 2B of* $\mathbb{M}$ *is a support class.*

Proof. We aim to show that the primitive permutation characters defined by the known maximal subgroups of $\mathbb{M}$ are sufficient to give us $\chi_{2B}(g) > 0$ for every $g \in \mathbb{M}$.

First note that $\mathbb{M}$ has only two classes of involutions (see the character table given in [8, p.220]) and so the centralizer of any involution contains 2B elements. Both the 2A and 2B centralizers are known to be maximal [8, p.228] and so the sum defining χ_{2B} must contain both of the permutation characters corresponding to these subgroups.

Now, let $g \in \mathbb{M}$ and suppose there exist elements $h, k \in \mathbb{M}$ $k \neq 1$ such that $g^a = h^b = k$ and h^c is in class 2B for some $a, b, c \in \mathbb{Z}^+$. Then $g, h \in C_{\mathbb{M}}(k)$, which must contain a 2B element. It follows that the sum defining χ_{2B} must contain the permutation characters defined by any maximal subgroups containing $C_{\mathbb{M}}(k)$. (For instance, if g is in class 119A then we can find an h in class 14B such that $k := h^2 = g^{17}$ which is in class 7A, so $a = 17$, $b = 2$ and $c = 7$ in this case. A maximal subgroup containing a 7A centralizer will therefore contain elements of class 119A and 2B and so the sum defining χ_{2B} must contain the permutation character corresponding to such a subgroup.)

Finally, from the fusion maps in the character table we see that the only classes not yet accounted for are the elements of orders 41, 59 and 71. It is known that $\mathbb{M}$ contains maximal copies of 41:40, $L_2(59)$ and $L_2(71)$ (see for instance [5, Table 1]). Furthermore, it is well known that the product of any two 2A elements of $\mathbb{M}$ has order at most 6. Since each of these subgroups only contain one class of involutions and in each of these subgroups there is a pair of involutions whose product is greater than 6, they must each contain 2B elements. It follows that the sum defining χ_{2B} must contain the permutation characters defined by each of these classes of maximal subgroups.

We thus have that $\chi_{2B}(g) > 0$ for all $g \in \mathbb{M}$, so 2B is a support class by Lemma 3. $\square$

Note we cannot replace 2B by 2A and improve this bound as this would give an 'upper bound' less than the lower bound of [4].

5. Acknowledgements

The author wishes to express his deepest gratitude to Professor Jamshid Moori for introducing him to the concept of spread in the first place and to the referee for making suggestions that resulted in substantial improvements to this paper.

References

[1] M. Aschbacher and R.M. Guralnick "Some Applications of the First Cohomology Group", J. Algebra, 1984, 90, 446-460
[2] G.J. Binder "The two-element bases of the symmetric group", Izv. Vysš. Učebn. Zaved. Mathematika, 90:9-11, (1970)
[3] J.D. Bradley and P.E. Holmes "Improved bounds for the spread of sporadic groups", LMS J. Comput. Math., 10, (2007), 132-140
[4] J.D. Bradley and J. Moori "On the exact spread of sporadic simple groups", Communications in Algebra, 35(8), 2588-2599, (2007)
[5] J.N. Bray and R.A. Wilson "Explicit construction of maximal subgroups of the Monster", J. Algebra, 300, (2006), 835-857
[6] J.L. Brenner and J. Wiegold "Two-Generator Groups, I", Michigan Math. J., (1975), 22, 53-64
[7] T. Breuer, R.M. Guralnick and W.M. Kantor "Probabilistic generation of finite simple groups II", J. Algebra, 320, (2008), 443-494
[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson "An ATLAS of finite groups", (Oxford University Press, 1985)
[9] S. Ganief and J. Moori "On the spread of the sporadic simple groups", Communications in Algebra, 29(8), 3239-3255 (2001)
[10] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; 2008, (http://www.gap-system.org)

[11] S. Garion "Connectivity of the product replacement graph of PSL(2,q)", J. Group Theory, 11, (2008), no. 6, 765-777
[12] R.M. Guralnick and A. Shalev "On the spread of finite simple groups", Combinatorica, 23, (1), (2003), 73-87
[13] A. Lucchini and A. Maróti "Some results and questions related to the generating graph of a finite group", Ischia group theory 2008 Proceedings of the conference in group theory, (2009), 183-208
[14] R.A. Wilson "The Maximal Subgroups of the Baby Monster, I", J. Algebra, 211, (1999), 1–14
[15] A. Woldar "The exact spread of the Mathieu group M_{11}", J. Group Theory, 10, (2007), 167-171

Department of Economics, Mathematics and Statistics, Birkbeck, University of London, Malet Street, London WC1E 7HX
E-mail address: bfairbairn@ems.bbk.ac.uk